

Management System: Information Resource Management

Subject Area: Computer Systems Management (Including Help Desk)

Procedure: 2 - Requesting User Accounts for EMCBC Employees (Federal or Contract)

Issue Date:
9/4/2012

Lead Subject Matter Expert:
Philip LaGamba

Management System Owner:
Ward Best

1.0 Applicability

This procedure applies to all Environmental Management Consolidated Business Center (EMCBC) Federal and contract employees accessing EMCBC Information Systems.

2.0 Required Procedure

The purpose of this procedure is to establish the process for requesting user accounts, rights, and access to specialized applications for EMCBC Federal and contract employees.

Step 1	<p>The Office of Human Resources representative, cognizant Assistant Director, or Federal Project Director notifies the Office of Information Resource Management (OIRM) of the new employee (User) and any known Special Access rights using the Computer Service Request (CSR) system. For instructions on CSR, see Procedure 1, <i>Computer Service Request (CSR)</i>.</p> <p>NOTE: The CSR system is used only to generate the account; the account will not be enabled without the completed Rules of Behavior for EMCBC Information Systems (User Agreement). In most cases, the new employee will not be available to complete the User Agreement until after the Start Date.</p>
Step 2	<p>OIRM creates a 30-day limited account.</p>
Step 3	<p>User completes Pages 1-3 of the Rules of Behavior for EMCBC Information Systems (User Agreement) and submits to supervisor to complete Page 4 (Additional Specific Access Rights for EMCBC Drives, Systems and Applications).</p> <p>NOTE: If Remote Access Connection service is required, User fills out the User Acknowledgement Agreement (UAA) for Two-Factor Authentication and Remote Access Connection Services and hand-carries to OIRM for identity proofing. After verification, a token is issued.</p>
Step 4	<p>Once the User Agreement is completed, the supervisor submits it to OIRM.</p>
Step 5	<p>OIRM verifies information, enables account, and provides User with credentials.</p>

Step 6	User logs in and completes Cyber Security Training within 30 days.
Step 7	OIRM removes 30-day limit from account and files the completed User Agreement.
Step 8	OIRM logs activity in IM Maintenance Log, as applicable.

3.0 References

- IMP-8308-001 – *Cyber Security – Account Management and User Responsibilities*
- [Procedure 1 – Computer Service Request](#)

4.0 Records Generated

Records generated through implementation of this procedure are identified as follows and are maintained by the Office of Information Management in accordance with the EMCBC Organizational File Plan.

Records Category Code	Records Title	Responsible Organization	QA Classification (Lifetime, Non-Permanent or N/A)
ADM 01-29.2-A3	Administrative Training Records – Cyber Security Training	Office of Information Management	N/A
GRS 24-03-B1	IT Asset and Configuration Management Files – User Agreements, Requests for User Accounts	Office of Information Management	N/A
GRS 24-08-C	IT Operations Records – Information Management Maintenance Log	Office of Information Management	N/A